UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/071,549	02/08/2002	Joseph J. Pantuso	NAI1P094/02.013.01	9867

28875 7590 04/22/2004

SILICON VALLEY INTELLECTUAL PROPERTY GROUP
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
ZAND, KAMBIZ	
ART UNIT	**PAPER NUMBER**
2132	10

DATE MAILED: 04/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/071,549	PANTUSO ET AL.	
	Examiner	Art Unit	
	Kambiz Zand	2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-29* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-29* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 February 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The text of those sections of Title 35,U.S.Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 1, 9, 13, 21 and 25-29 have been amended.
4. Claims 1-29 are pending.

Drawings

5. Figure 2 and 4-6 should be designated by a legend such as --Prior Art-- because only that which is old is illustrated. See MPEP § 608.02(g). A proposed drawing correction or corrected drawings are required in reply to the Office action to avoid abandonment of the application. The objection to the drawings will not be held in abeyance.

   As per Fig.2, please see fig.1a of U.S. Patent number 5,812,668; Applicant claims that fig.4-6 represent various traffic events in accordance with fig.3 flowchart (see page 11, lines 5-6; page 12, lines 11-12 and page 13, lines 1-2 of the specification). However it is clear that fig.4-6 display MCAFEE PERSONAL FIREWALL PLUS Internet application.

Response to Arguments

6. Applicant's arguments with respect to Maloney fails to teach the display of the world map filed 03/31/04 have been fully considered but they are moot in view of new ground(s) of rejection.

7. As per Applicant arguments that node representation by Maloney is a tree-based, suggesting that Applicant's claim invention does not display tree-based node, Examiner refers Applicant to the following remarks:

Examiner considers displaying of a map where traces utilizing firewall shown as tree-based nodes where the event from one node to other where the traces has been detected is being display. However Examiner suggests if there is a specific difference in that regards, then such differences should be presented in the claim language in a manner that shows such a differences in a clear and concise language over prior art of record.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention

was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. **Claims 1-29** are rejected under 35 U.S.C. 103(a) as being unpatentable over Maloney et al (6,269,447 B1) in view of Dev et al (5,261,044 A).

As per claims 1, 13 and 25 Maloney et al (6,269,447 B1) teach a method, a computer program product and a system for tracing a traffic event utilizing a firewall (see fig.6, item 54), comprising:

(a) executing a firewall on a local computer (see fig.6, item 54; fig.7, items 74 and 76 where item 74 acts as executed firewall on local computers within the network 64, 66,68 or other local computers 70 or 72);

(b) monitoring traffic events between the local computer and remote computer over a network utilizing the firewall (see fig.7, item 74 that monitors traffic events between any local computer in network 64 and remote computers of network 66 or vice versa; abstract; col.1, lines 57-67 and col.2, lines 1-28);

(c) displaying the traffic events utilizing the firewall (see col.2, lines 12-15);

(d) tracing at least one of the traffic events utilizing the firewall (see col. 2, lines 12-15 where one of the tracing events may be normal or up normal usage patterns); and

(e) displaying a map with an illustration of the trace thereon utilizing the firewall (see col.11, lines 39-67 and col.12, lines 1-2 where after the analysis of an event map of the trace is displayed). Also see col.4-11 and col.12, lines 1-34 for detailed description of the above/below limitations but do not explicitly disclose displaying a world map of network events. However Dev et al (5, 261,044 A) display a network world map of

network events and different views within the map (see col.13, lines 12-29 where multiple views of network is displayed including a map of the world that is called highest level view). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Dev et al multiple view such as world map view in Maloney's information security analysis and monitoring network system in order to have a broad and narrow LAN/WAN monitoring in either a passive and/or active mode with respect to network events within a world map or region or a location within the network that is being monitored.

As per claims 2 and 14 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 1 and 13, wherein the traffic events are displayed in an event log (see col.6, lines 63-67 and col.7, lines 1-19 where the data are gathered are considered as event log that keep track of events within the network traffic; col.5, lines 33-38).

As per claims 3 and 15 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 2 and 14, wherein the event log identifies a time (col.2, lines 27-29) and Internet protocol (IP) address associated with the traffic events (see col.4, lines 65-67).

As per claims 4 and 16 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 2 and 14, wherein the traffic events are organized based on times the traffic events are logged (see col.2, lines 27-29).

As per claims 5 and 17 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 2 and 14, wherein the traffic events include attempts to access the local computer (see col. 4, lines 47-53).

As per claims 6 and 18 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 1 and 13, wherein the at least one traffic event is traced in response to a user request (see col.11, lines 18-26 where user is able to negotiate a display of event trace).

As per claims 7 and 19 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 1 and 13, wherein the tracing includes identifying a plurality of network segments traversed by the traffic event (see fig.6 and 7).

As per claims 8 and 20 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 7 and 19, wherein the map includes the network segments (see col.4, lines 19-26).

As per claims 9 and 21 teach the method, a computer program product as recited in claims 8 and 20, and further comprising displaying a plurality of views (see col.5, lines 7-65).

As per claims 10-12 and 22-24 Maloney et al (6,269,447 B1) teach the method, a computer program product as recited in claims 9-11 and 21-23, wherein a geographical location of the network segments is displayed upon the selection of a first one/second one and the third one of the views (see col.5, lines 7-65).

As per claim 26 Maloney et al (6,269,447 B1) teach a system for tracing a traffic event utilizing a firewall (see fig.6, item 54), comprising:

(a) executing a firewall on a local computer (see fig.6, item 54; fig.7, items 74 and 76 where item 74 acts as executed firewall on local computers within the network 64, 66,68 or other local computers 70 or 72);

(b) monitoring traffic events between the local computer and remote computer over a network utilizing the firewall (see fig.7, item 74 that monitors traffic events between any local computer in network 64 and remote computers of network 66 or vice versa; abstract; col.1, lines 57-67 and col.2, lines 1-28);

(c) displaying the traffic events utilizing the firewall (see col.2, lines 12-15);

(d) tracing at least one of the traffic events utilizing the firewall (see col. 2, lines 12-15 where one of the tracing events may be normal or up normal usage patterns); and

(e) displaying a geographical location of the network segments associated with the traffic events on a map upon the selection of a first one of a plurality of views utilizing firewall (see col.5, lines 7-65).

(f) displaying a plurality of nodes of the network segments upon the selection of a second one of the views utilizing firewall (see col.5, lines 7-65); and

(g) displaying a plurality of nodes of the network segments upon the selection of a third one of the views utilizing firewall (see col.5, lines 7-65).Also see col.4-11 and col.12, lines 1-34 for detailed description of the above limitations but do not explicitly disclose displaying a world map of network events. However Dev et al (5, 261,044 A) display a network world map of network events and different views within the map (see col.13, lines 12-29 where multiple views of network is displayed including a map of the world that is called highest level view). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Dev et al multiple view such as world map view in Maloney's information security analysis and monitoring network system in order to have a broad and narrow LAN/WAN monitoring in either a passive and/or active mode with respect to network events within a world map or region or a location within the network that is being monitored.

As per claim 27 Maloney et al (6,269,447 B1) teach a method for tracing a traffic event utilizing a firewall (see fig.6, item 54), comprising:

(a) executing a firewall on a local computer (see fig.6, item 54; fig.7, items 74 and 76 where item 74 acts as executed firewall on local computers within the network 64, 66,68 or other local computers 70 or 72);

(b) monitoring traffic events between the local computer and remote computer over a network utilizing the firewall (see fig.7, item 74 that monitors traffic events between any local computer in network 64 and remote computers of network 66 or vice versa; abstract; col.1, lines 57-67 and col.2, lines 1-28);

(c) logging the traffic events in an event log utilizing the firewall, wherein the event log identifies a time (col.2, lines 27-29) and internet protocol (IP) address associated with the traffic events (see col.4, lines 65-67).

(d) organizing the traffic events in the event log based on times the traffic events are logged utilizing the firewall (see col.2, lines 27-29).

(e) displaying the traffic events utilizing the firewall (see col.2, lines 12-15);

(f) detecting the selection of one of the traffic event by a user ().

(g) tracing at least one of the traffic events utilizing the firewall upon the selection thereof, wherein the tracing identifies a plurality of network segments traversed by the traffic event (see col. 2, lines 12-15 where one of the tracing events may be normal or up normal usage patterns).

(h) detecting the selection of one of a plurality of views by the user (see col.11, lines 18-26 where user is able to negotiate a display of event trace); and

(i) displaying the network segments in the selected view upon the selection of one of the views, wherein one of the views includes a map with an illustration of a trace thereon

(see col.5, lines 7-65).Also see col.4-11 and col.12, lines 1-34 for detailed description of the above limitations but do not explicitly disclose displaying a world map of network events. However Dev et al (5, 261,044 A) display a network world map of network events and different views within the map (see col.13, lines 12-29 where multiple views of network is displayed including a map of the world that is called highest level view). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Dev et al multiple view such as world map view in Maloney's information security analysis and monitoring network system in order to have a broad and narrow LAN/WAN monitoring in either a passive and/or active mode with respect to network events within a world map or region or a location within the network that is being monitored.

As per claims 28 and 29 Maloney et al (6,269,447 B1) teach a method, a computer program product for geographically tracing event utilizing a personal firewall, comprising: monitoring traffic events between a local computer and a remote computer over a network utilizing a personal firewall (see fig.7, item 74 that monitors traffic events between any local computer in network 64 and remote computers of network 66 or vice versa; abstract; col.1, lines 57-67 and col.2, lines 1-28):
Displaying the traffic events in a map an event log utilizing the personal firewall (see col.2, lines 12-15), wherein the traffic events are organized based on a time associated therewith (see col.2, lines 27-29);

Tracing at least one of the traffic events utilizing the personal firewall (see col. 2, lines 12-15 where one of the tracing events may be normal or up normal usage patterns), wherein the at least one traffic event is traced in response to a user request (see col.11, lines 18-26 where user is able to negotiate a display of event trace).Also see col.4-11 and col.12, lines 1-34 for detailed description of the above limitations but do not explicitly disclose displaying a world map of network events. However Dev et al (5, 261,044 A) display a network world map of network events and different views within the map (see col.13, lines 12-29 where multiple views of network is displayed including a map of the world that is called highest level view). It would have been obvious to one of ordinary skilled in the art at the time the invention was made to utilize Dev et al multiple view such as world map view in Maloney's information security analysis and monitoring network system in order to have a broad and narrow LAN/WAN monitoring in either a passive and/or active mode with respect to network events within a world map or region or a location within the network that is being monitored.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

U.S.Patent No. US (5, 812, 668 A) teach system and method for verifying of the operation of a remote transaction clearance system.

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kambiz Zand whose telephone number is (703) 306-4169. The examiner can normally reached on Monday-Thursday (8:00-5:00). If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned as (703) 872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR

or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Kambiz Zand

04/12/04

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100